(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 July 2001 (19.07.2001)

PCT

(10) International Publication Number
WO 01/52205 A1

(51) International Patent Classification[7]: G07F 7/10, 7/08

(21) International Application Number: PCT/IE01/00004

(22) International Filing Date: 12 January 2001 (12.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0065003.7 12 January 2000 (12.01.2000) EP
S2000/0468 9 June 2000 (09.06.2000) IE

(71) Applicant *(for all designated States except US)*: **SEAGLADE DEVELOPMENTS LIMITED** [—/IE]; 1st floor, Nathan House, Christchurch Square, Dublin 8 (IE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MEAGHER, Philip** [—/IE]; "Irie Blue", Barnaran, Rathangan, County Kildare (IE).

(74) Common Representative: **MEAGHER, Philip**; "Irie Blue", Barnaran, Rathangan, County Kildare (IE).

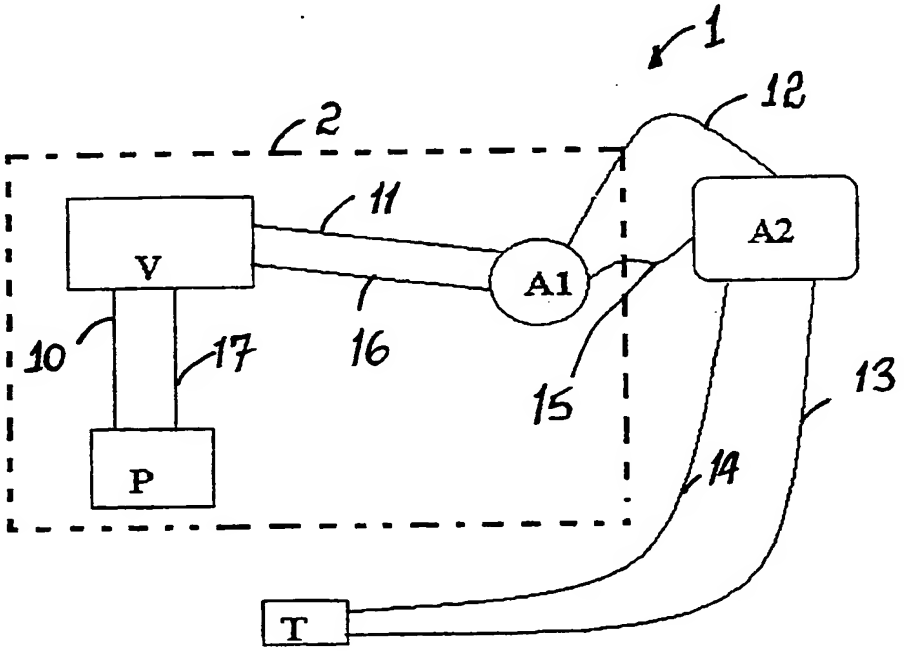
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: A PROCESSING METHOD AND APPARATUS



(57) Abstract: A method and apparatus for generating a telephone call from an authentication server to a credit card user to validate a transaction. The server retrieves a telephone number and Personal Identification Number (PIN) when a transaction request is received and when the user enters the correct PIN generates an authentication code based on the transaction and the PIN to validate the transaction. The invention prevents fraudulent use of the card and guarantees all transactions.

WO 01/52205 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A PROCESSING METHOD AND APPARATUS

The present invention relates to a processing system and apparatus for use in processing credit card transactions. The invention is particularly, but not exclusively suited for use in an electronic commerce environment.

The term "credit card" as used herein is intended to include debit cards, voucher cards and any other real or virtual transaction media used to substitute cash or authenticate the legitimacy of a purchase.

The business of selling products and services across communication channels, such as the Internet, is now generally referred to as electronic commerce or "E Commerce". Widespread acceptance of E Commerce has not been forthcoming because of legitimate user security concerns. These concerns relate to potential fraud that may be perpetrated against purchasers, vendors or even card issuing financial institutions.

Cards, which have been lost or stolen account for the majority of fraudulent use, however, this use is usually quickly discovered by the user and is easily remedied by cancellation of the card. Additionally, many credit card suppliers perform analysis of purchasing patterns and can identify a stolen card that has not been reported by a radical change in spending. The potential losses to fraud, while often limited for the card holder, are significant to vendors and to card issuing authorities. In most instances the card issuing authorities are forced to rely on the diligence of the card holder to report a theft. Purchase pattern analysis is not an exact art and it may take a significant period for the card authority to detect aberrant spending patterns. Furthermore, the experienced fraudster is generally aware that low level purchases are significantly less likely to be detected than extravagant ones.

In the E Commerce environment where there is no face to face transaction the fraud is easier to perpetrate and can remain undetected for a much longer period. To perpetrate credit card fraud in this arena a criminal normally requires only three data components for credit card transactions, namely the cardholders name, the credit card number and the expiry date. As billing addresses are rarely verified, with this information alone the criminal is free to go "on-

line" and make illegal purchases. The criminal can obtain this information in numerous ways. The necessary information is regularly printed on credit card receipts and carbon copies and therefore if a criminal obtains a carelessly discarded receipt there is significant potential for fraud both through E Commerce and telesales transactions. By the nature of existing transactions, there are at least two copies of the relevant information available for each transaction, namely, the vendor's copy and the purchaser's copy. Additional copies are often made for the card issuing authority. Where carbon slips are produced, additional material is available for the potential fraudster. It will thus be seen that there is a significant amount of material available, over which the card holder has no control which can be put to fraudulent use. People to whom the credit card information has been given legitimately may also obtain the necessary information. For example, a dishonest staff member in a shop, hotel or restaurant can record the credit card number for subsequent use. This is often referred to as "compromised numbers" fraud.

Another form of credit card fraud is that associated with overcharging by unscrupulous vendors. This may occur by way of a direct charge above an agreed amount, an accidental or deliberate double billing or indeed by a service provider periodically and automatically re-billing the card when not authorised. These risks are particularly pertinent to credit card holders who have relatively high spending limits, in that if fraud should occur, it may be some time before it is detected. Indeed it is possible for low-level fraud to continue undetected if a senior member of staff in a company holds the card where the bill is automatically paid by an accounts department.

Irrespective of how the fraud is carried out there is significant potential for cardholder embarrassment as counterfeit use of the credit card may not become apparent for some time and may lead to refusal of a transaction. Additionally, when fraud does occur the consumer is required to persuade the credit card supplier that fraud has indeed occurred. This may be particularly difficult to prove if the card holder has lost or had stolen a purse or wallet containing the card and a collection of receipts. The fraudulent use can follow substantially the pattern of previous use from the receipts.

Many solutions have been proposed to these problems, however, known solutions suffer from

some or all of the limitations mentioned above. Ideally, the solution would be to obtain the functionality of a credit card, while ensuring the authenticity of all transactions. Obviously reporting card theft and elaborate verification of altered purchasing patterns do not provide this security. Similarly, the provision of disposable cards of predetermined maximum value or disposable codes while limiting exposure, do not adequately secure transactions.

The Secure Electronic Transaction (SET) protocol defined by leading computer companies and the credit card industry for electronic transmission of credit card details via the Internet is also limited. While SET does provide a detailed protocol for encryption of credit card details and verification of participants in an electronic transaction it is still open to abuse and represents a challenge to criminals to obtain the information required to carry out fraud. SET type solutions are also in direct competition with specific electronic transaction systems such as "Check Free", "Cyber Cash" and "First Virtual" and this leads to the emergence of incompatible format competing technologies. The existence of a multiplicity of these technologies will be likely to deter both traders and consumers unless a dominant force emerges. Similarly, many of these systems require modifications of the technology used at the point of sale, which will require considerable investment and further limit the uptake of the systems.

Another solution to these problems has been proposed by Millicom International Cellular and is marketed under the name GiSMo. The GiSMo system operates as follows:-

a purchaser requests an order form a vendor on a data channel;

upon receiving the request, the vendor retrieves and transmits the order form to the purchaser again on the data channel;

the user completes the order form received from the vendor and transmits the purchase request to a GiSMo server;

the GiSMo server then responds by sending a purchase specific identification number (PSIN) code for that purchase to the purchasers pre-defined telephone

number using a Short Messaging Service (SMS) message;

the user receives this PSIN code and returns the PSIN code using the data channel to the GiSMo Server;

GiSMo then issues the user with a digital receipt across the data channel; and

the account is finally settled between GiSMo and the vendor.

While undoubtedly representing a significant improvement over conventional E Commerce payment methodologies, there are a number of technical and commercial problems with this solution both in terms of security and viability. Each vendor site wishing to use this system must subscribe to the GiSMo service to obtain the appropriate software to process payments. As there is no dominant system of this type vendors have to date been reluctant to sign up for such services. Furthermore, existing credit card companies have resisted attempts by third parties to interpose themselves as Virtual charge card authorities on any significant scale. Installation of appropriate GiSMo software on each and every vendor site is required. Given the number of Web sites offering products or services currently in existence the time and cost of manually changing all of these sites means that large scale implementation is not feasible. Site owners are reluctant to re-develop their web sites to accommodate GiSMo type forms both because of the cost implication and the lack of guaranteed returns. Even where sites do incorporate GiSMo type forms they are compelled to maintain conventional payment forms to accommodate non-GiSMo customers.

Another problem arises in that payment using GiSMo type systems can only be made to vendor sites, which incorporate GiSMo software. This significantly limits the number of sites on which the customer may shop, which is obviously unacceptable. A more appropriate solution will be one which operates independently of the vendor site, where there is no requirement for modification to existing, under-construction or planned web sites. Vendors in such a solution will not be bound to a given customer base and will not be required to make modifications to existing payment strategies. The net technical saving

both in storage capacity across the net, business restriction and portability will represent a significant improvement over GiSMo and other systems of this type.

The delivery of a PSIN number to a GSM phone in the GiSMo disclosure represents an inherent risk and limitation. If the GSM phone is stolen then a purchase notification delivered to the phone thief can be authenticated back to GiSMo and allow the transaction to be processed. Furthermore, SMS messages are often stored in telephone memory and can be retrieved with relative ease. Thus, the theft of the phone is equivalent to the theft of a credit card and offers no additional security. While timely detection of the phone theft is advantageous in limiting fraudulent use it is no better than discovering the theft of an actual credit card and further has the limitation of only operating on GiSMo sites and being operable only by GiSMo customers. The limitation of the GiSMo system arises from the requirement of the user to have access to both a data channel and the telephone thus, a user cannot avail themselves of telesales services. For example, a user cannot telephone for cinema tickets and return confirmation.

As the GiSMo site is directly attached to the Internet it is as susceptible to attack by hackers as any other site. Skilled fraudsters may access the list of authentication PSINs or functions for obtaining these codes. Even if the functions for generating the GiSMo PSIN are frequently changed, the realistic possibility exists for the ubiquitous hacker to change one or more previously specified telephone numbers to a number which the fraudulent user may manipulate.

The system described in GiSMo has another security risk in that the passive cancellation of the order by failure to respond to the SMS message transmitted is not a true authentication feedback loop. Positive confirmation to confirm the authenticity of a given transaction is more secure as, while unlikely, interception of the transmitted SMS in the GiSMo system could permit fraudulent use.

The present invention is directed towards overcoming the aforementioned problems.

It is a particular objective of the present invention to enhance security of "card not present"

transactions, including Internet/E Commerce transactions and telesales. The invention applies equally to enhancing the security of "card present" transactions to reduce the level of fraud and particularly to attenuate losses through fraud currently borne predominantly by the card issuing authorities.

Accordingly there is provided a method and or apparatus in accordance with the invention for use with a credit card in a commercial environment of the type having

a purchaser interface, through which order transactions are placed for goods or services using credit card data,

a vendor interface for receiving placed orders, the vendor interface further having means for authenticating the legitimacy of the placed order, by communicating credit card data and order data to an authentication authority and receiving an authentication code for an approved transaction,

characterised in that method and or apparatus further incorporates means for controlling communication between the authentication authority and a credit card user in response to the order transaction.

In this way, before any transaction is processed, the user must first validate the authenticity of the request rather than merely being informed after the fact that a transaction has been processed.

Preferably, the means for authenticating the legitimacy of the placed order comprises a first authentication server and a second authentication server.

In one arrangement, communication between these servers is encoded.

Preferably, the second authentication server accepts requests in a predetermined frame format only.

In a particularly preferred arrangement, the second authentication server incorporates a computer telephony interface (CTI) for generating a phone call to a user specified telephone number.

Ideally, the second authentication server incorporates means for generating an audio message for transmission to the user.

Preferably, the second authentication server incorporates means for receiving a personal identification number (PIN) from the user and means for comparing the received PIN with a predefined PIN.

Ideally, the second authentication server incorporates means for generating an authentication code based on a periodically alterable algorithm, a user identifier, a vendor identifier, date and time.

In this way it will be understood that no transactions will be processed by the credit card issuing authority without the generated code and therefore will cease. For example the fraudulent practice known as "skimming" in which the credit card is swiped twice will generate two calls to the user and will be immediately apparent. Additionally, unscrupulous vendors will realise that automatic re-billing of the credit card will generate a call and will be declined by the user if the product or service is no longer required.

For second user or authorised user cards, the primary user may select whether the generated telephone call is directed to the primary user or the second user/authorised user.

Another benefit of the card is that parents or guardians can give user cards to minors in their care with confidence. If the minor requests authorisation for a frivolous or excessive purchase the parent or guardian can decline the transaction. On the other hand, legitimate purchases can be validated. In addition to this flexibility, the use of these cards will be helpful in prevention of theft by bullies.

The card of the invention will also be useful to purchasing managers who can issue individual

cards, departmental cards or can generally issue the office card number. The manager can then specify contact criteria on each account or on the general account. For example, the manager may request that verification contact be made for an individual item in excess of a certain amount. They may equally request contact when a budgeted amount is exceeded in a certain period or when a good or service transaction is received outside of a given set of products or services specified.

Advantageously, the user specified telephone number is to a mobile telephone. The user thus makes verification by transmitting the PIN number. As the PIN is manually entered rather than retained in telephone memory, it obviates the disadvantages considered above where a fruadster has access to both stolen phone and card details.

Ideally, the second authentication server incorporates means for generating calls through the CTI in response to these conditions.

In a particularly preferred arrangement, the second authentication server incorporates means for automatically generating a response telephone box in response to and unanswered call and storing the generated message in the box.

In one embodiment, the box is formed for reception of the PIN asynchronously.

Thus, when a call to verify a transaction cannot be completed the message may be stored and the user contacted using a subsequent message or using a Short Messaging System (SMS) formatted code with a number identifying the box.

According to one aspect of the invention there is provided a method for authenticating credit card transactions including the steps of: -

identifying a purchase request;

extracting customer details associated with the request;

extracting vendor details associated with the request;

generating a confirmation call to a user to validate the purchase request;

receiving an authentication signal from the user; and

generating a unique authentication code based on extracted data and timestamp information.

Preferably, the method further incorporates the steps of retrieving a customer code associated with an account and transmits this information across a secure line or encrypts the information to an independent network .

A method and or apparatus formed or operated in accordance with the invention has a number of distinct advantages over known solutions. As no software resides on vendor sites, there is no limitation to the number and or hardware on which the invention can operate conveniently facilitating implementation and acceptance. Positive confirmation from the user for each purchase eliminates the risk of fraudulent use as the user confirms and a device does not provide confirmation. Automatic call back when the credit card is not presented significantly reduces staff or operating system requirements. Furthermore there is no subjective decision making required. As the call back facility is not accessible from the Internet there is no risk that the mechanism will be hacked by fraudsters. Furthermore, users of the invention are not bound to a specific card issuer or sites with appropriate software.

Further characteristics and advantages of the processing method and apparatus according to the invention will become clear in the course of the detailed description which follows with reference to the appended drawings, provided by way of a non-limiting example, in which:

Fig. 1 is a diagrammatic view of an E Commerce environment operating in accordance with the method of the invention; and

Fig. 2 is a flow diagram illustrating the steps of the method.

For the purposes of this description, specific system architectures, processors, memory devices, encryption methodologies, communication channels, protocol formats, interfaces, operating systems, timing and performance details have been omitted in order not to unnecessarily obscure the present invention. Thus the constituent components of the invention have been described in terms of functionality, as many ways of achieving said functionality will be readily apparent to those skilled in the art.

Referring to the drawings and initially to Fig. 1 there is illustrated in an E Commerce environment in accordance with the invention indicated generally by the reference numeral 1. The component elements of the environment 1 are divided into those elements operating within the Internet shown by the interrupted line 2 and those elements outside of the Internet 2. The elements of the invention operating within the Internet 2 are a purchaser interface P, a vendor interface V and a first authentication server A1. The elements operating outside of the Internet 2 are a second authentication server A2 and a telephone T.

Referring now to Fig. 2 operation of the various components described in relation to Fig. 1 will be more clearly understood from the flow chart illustrating the method of the invention. Before the method of the invention can be implemented a number of steps are required. Firstly a potential user of the system makes an application to the credit card company for approval as a client and for issuance of a credit limit. On the application the user specifies a telephone number and a personal identification number (PIN). Providing the applicant is successful and is accepted as a client of the credit card company a card is then issued in the normal way and operates in common with normal credit card operations. This credit card can be used in conventional face-to-face transactions, however, it is important to note that a particular feature of this credit card is that first four digits of the sixteen digit credit card number which are normally used to identify the type of credit card being used are different to those which are normally used. It is important for potential fraudulent users of the card to be made aware that this is a credit card with inherent "security".

Having obtained a credit card the user can generate a purchase request in step 1. This purchase request is transmitted to the vendor interface V through the purchaser interface P as is currently performed in E Commerce transactions. The purchase request may include details of the goods or services being purchased and the price of those goods or services. The purchase request will also include the customer's card number with the identifying four digits. The transmission of this information to the vendor interface V is shown in Fig. 1 by the reference numeral 10.

On receipt of the purchase request the vendor transmits an authentication request to an authentication authority within step 2. The transmission is identified in Fig. 1 by the reference numeral 11. The authentication authority comprises the first authentication server A1 and the second authentication server A2. In step 3 the authentication server A1 performs the normal credit verification process to establish whether the user that generated the initial purchasing request has sufficient available credit balance to allow this request to continue. In order not to unnecessarily obscure the present invention, the mechanics of this verification are not described and do not form part of this invention. When the verification of available credit balance and conformation of the fact that the credit card has not been reported stolen are received the first authentication server A1 generates a frame format message for transmission to the second authentication server A2 in step 4. (Numeral 12 in Fig. 1). It is an important feature of the current invention that this frame format message is generated only when the card is not physically presented during the transaction. Monitoring a "card not presented" or "card not present" field in the conventional validation described achieves this.

Another important feature of this invention is that the second authentication server A2 is outside of the Internet and is therefore not susceptible to malicious computer interference called "Hacking". The second authentication server A2 will only accept communications from the first authentication server A1 in a predefined format. It is important to appreciate therefore that interrogation requests to the authentication server A2 will not be processed as the only acceptable format of information transmission to the second authentication server A2 will contain a code relating to the particular customer who generated the initial request, an identification of the vendor, an identification of the products or service

purchased and details of the cost of that product or service. This information may be encrypted and will in one aspect of the invention not be clearly identifiably related to the credit card number. On receipt of a validly formatted authentication request from the first authentication server A1 the second authentication server A2 in step 5 retrieves from a list of customers the telephone number and PIN number specified on initial setup of the account. An automatic dialer forming part of the second authentication server then dials the retrieved telephone number in step 6 (numeral 13 in Fig. 1) and an automatically generated message is played to the telephone when answered. This message will identify the name of the vendor, the product or service being purchased and the cost as identified in the initial purchase request and relayed by the vendor interface V. Typically, this message will take the format of a spoken message saying

> *"You have requested authorisation for*..... **product or service** ..... *from* ..... **vendor**..... *at* ..... **currency value**..... *please enter your PIN number to verify transaction"*.

The user can then enter the PIN number specified on initial setup of the account in step 6 (Numeral 14 Fig. 1) to authenticate the purchase request or alternatively enter 0 to cancel the transaction. On receiving a valid PIN number the authentication server 2 generates an encrypted authentication code being a function of the vendor identification, user identification, time and date in step 7. This code may then be encrypted for retransmission to the first authentication server A1 in step 8 (Numeral 15 of Fig. 1).

The various methods of fraudulent use of credit cards above are therefore eliminated, as vendors are aware that double billing or automatic rebilling of the credit card will immediately cause a telephone call to be placed to the user. Similarly it will not be possible for an unscrupulous vendor to double bill using the original authentication as the credit card supplier in charge of the authentication servers A1, A2 will not process transactions unless accompanied by a valid code. This code relates as described as above to the user ID, vendor ID time and date. The first authentication server transmits this code together with an approval purchase order to the vendor (Step 8 and numeral 16 of Fig. 1) and the vendor may optionally notify the purchaser of acceptance of the purchase order

(Step 9 and numeral 17 of Fig. 1).

As all transactions will be notified to the user of the card it is possible, for example, for a parent to give a credit card to a child where this was previously not possible. In the circumstances where a child uses the card legitimately the parent or guardian will have no problem is validating these legitimate purchase requests. However, if a child uses the credit card to purchase an item of which the parent or guardian does not approve the request can be declined. Particularly, where the authorised user card is issued to a minor its use for "card not present" transactions can be disabled. Thus, the card cannot be used to gain access to protected or adult only information or presentations, for example, premium rate fanzine sites or adult only sites on the Internet.

In the event that the telephone number being called by the second authentication server A2 is engaged or otherwise unreachable the system can be defined to recall the number within a predefined time period and continue recalling until an answer is obtained.

When a call is answered by some automatic means such as a telephone answering machine or message minder a telephone number can be generated to which the user can telephone to authenticate the transaction request at a later stage.

It is anticipated that the use of GSM standards to extract caller identification number may be used in further verification of the transaction processing request. In any event, the PIN number for the credit card may be taken as general authorisation to proceed with the transaction.

Another feature of this invention is the ability of the system to be modified for use by purchasing managers. For example, if an organisation has many individuals who are authorised to purchase set amounts of materials or supplies in a given period a single credit card number can be made available for such electronic purchases. The account can be modified so that a single source is contactable to validate purchasing requests and the details of this account may specify the purchase requests below a given financial value are automatically authorised without reference to the authority.

The present invention facilitates further enhancements to existing spending pattern recognition paradigms by allowing the card user provide additional information to the card issuing authority. By providing protected access to a card holder's profile, the card holder can in advance validate new standing orders, identify an irregular or high value purchase and can authorise transfers from one account to another.

Using such techniques, the incidence if validating or authentication traffic over communication channels may be minimised.

If a user has gained access to their personal card spending profile, the user can set automatic reference limits. For example, if the card holder or authorised user makes regular high value purchases at one venue such as £400 at a supermarket, then this transaction can be "de-selected" from the pattern checking regime. If an upper spending limit were exceeded (say £500 in the above case), the card holder would be contacted at the time of the transaction. This arrangement will become increasingly more useful as the number of individuals shopping from home via the Internet or Interactive Television increases.

The use of the present invention in "card present" transactions is of particular value to the card holder, vendor and card issuing authority when considering high value purchases from jewelry and fashion clothes to vehicles. Often such purchases are impulsive and the card owner will wish to retain the facility to make purchases up to the established credit limit applied to the credit card. In such instances authentication or validation communications will be initiated. For high value purchases which are planned, the approximate value of the transaction may be entered in the card holder's profile for a particular date.

Changes in spending patterns can also be anticipated and authorisation communications suppressed for a pre-determined period to account for overseas spending while on business trips or annual vacation. For company credit cards, when the card user is overseas, the PIN may be provided from the company office or by a trusted representative of the company, such as the financial director or accounts department staff only.

Currently, credit card issuing authorities do not issue cards to minors and in many cases it is illegal to do so. With current market trends, the value of the teenage and minors market is increasing annually and there is a likely requirement for credit cards to meet spending demands and to reduce the risk of robbery assaults on minors.

While the provision of emergency funds or a spending allowance on a debit card or by voucher scheme is sufficient in some circumstances, it does not allow the flexibility and spending scope associated with a credit card. The issuance of a credit card to a minor may become an acceptable service if certain provisions were set in place. Primary of these, certainly in the United States, would be the restriction on the use of these cards to gain access to "adult material" sites and services via the Internet. This could be most easily realised by withdrawing the provision of "card not present" transaction facilities for cards issued to minors.

The term "timestamp" as used in this specification is directed to manual, mechanical and electronic signatures recording either or both of data and time.

It will be understood that the invention described above with reference to the use of a credit card may equally well be used with a charge card, debit card or virtual payment system.

It will be further understood that the authentication server may also incorporate the functionality of a firewall or tailored firewall.

The invention is not limited to the embodiments hereinbefore described which may be varied in both construction and detail.

Claims

1. A processing system for use in processing credit card transactions, the system being of the type having a purchaser interface, for generating an order transaction incorporating credit card data, a vendor interface for receiving the generated order transaction and having means for authenticating legitimacy of the generated order transaction, by communication with an authentication authority to receive an authentication code for an approved transaction characterised in that the system further incorporates means for automatically controlling communication between the authentication authority and a credit card user in response to the generated order transaction for card not present identified transactions.

2. A processing system as claimed in claim 1, in which the means for means for automatically controlling communication is provided by a second authentication server formed for encoded communication in a predetermined frame format with the authentication authority.

3. A processing system as claimed in claim 1 or claim 2, in which the second authentication server incorporates a computer telephony interface (CTI) for automatic communication with the credit card user using unique predefined communication data stored in the second authentication server.

4. A processing system as claimed in claim 3, in which the computer telephony interface is formed for automatic generation of an audio message for transmission to the credit card user.

5. A processing system as claimed in any of claims 2 to 4, in which the second authentication server incorporates means for receiving a personal identification number (PIN) from the credit card user during communication between the authentication authority and a credit card user in response to the order transaction and means for comparing the received PIN with a predefined PIN stored on the second authentication server.

6. A processing system as claimed in claim 5, in which the second authentication server incorporates means for automatically generating an authentication code in response to a matched PIN condition based on a user identifier, a vendor identifier, timestamp and transaction value.

7. A processing system as claimed in any preceding claim, in which the means for automatically controlling communication between the authentication authority and a credit card user in response to the order transaction further incorporates means for automatically generating a response telephone box and for communicating a telephone box location to the credit card user.

8. A processing system as claimed in any of claims 2 to 7 wherein the second authentication server incorporates a tailored firewall.

9. A processing method for authenticating credit card transactions including the steps of: -

identifying a non face to face, card not present purchase request with an associated cost and product code identifying a purchase request;

extracting customer details from the identified request;

extracting vendor details from the identified the request;

automatically generating a confirmation call to a user to validate the purchase request in response to the identified purchase request;

requesting and receiving a predefined authentication signal from the user; and

generating a unique authentication code based on extracted data and timestamp information.

10. A processing method as claimed in claim 9 further incorporating , prior to the automatic call generation, the steps of :-

retrieving a customer code associated with extracted customer details;

generating a fixed length frame formatted message incorporating the customer code, transaction value product code and extracted vendor details; and

transmission of the fixed length a frame formatted message to a second authentication server.

11. A processing method as claimed in claim 10, in which the step of automatically generating a confirmation call to a user to validate the purchase request incorporates retrieving a unique predefined contact location and validation data for the customer code of the frame formatted message.

12. An authentication server for processing credit card transactions, the server having:-

a vendor interface for receiving an order from a vendor;

processing means for detecting a card not present flag in the received order; and

means for authenticating legitimacy of the received order,

characterised in that the means for authenticating legitimacy of the received order incorporates means for initiating communication with a credit card user in response to the detected card not present flag, requesting a predefined verification code from the user and means for identifying an authentic verification code to enable processing of the transaction.

13. An authentication server as claimed in claim 12, in which the means for initiating communication with a credit card user is provided by a second authentication server formed for encoded communication in a predetermined frame format with the authentication server.

14. An authentication server as claimed in claim 12 or claim 13, in which the second authentication server incorporates a computer telephony interface (CTI) for automatic communication with the credit card user using unique predefined communication data stored in the second authentication server.

15. An authentication server as claimed in claim 14, in which the computer telephony interface is formed for automatic generation of an audio message for transmission to the credit card user.

16. An authentication server as claimed in any of claims 13 to 15, in which the means for identifying an authentic verification code incorporates means for receiving a personal identification number (PIN) from the credit card user and means for comparing the received PIN with a predefined PIN stored on the second authentication server.

17. An authentication server as claimed in claim 16, in which the second authentication server incorporates means for automatically generating an authentication code in response to a matched PIN condition based on, a user identifier, a vendor identifier, timestamp and transaction value.

18. An authentication server as claimed in any of claims 12 to 17 in which the means for automatically controlling communication between the authentication server and a credit card user in response to the order further incorporates means for generating a response telephone box and for communicating a telephone box location to the credit card user.

19. A processing system for verification of credit card transactions, having a vendor

interface for receiving an order from a vendor and means for authenticating legitimacy of the received order, characterised in that the means for authenticating legitimacy of the received order is provided by a first authentication server connected to the vendor interface and a second authentication server formed for encoded communication in a predetermined frame format with the first authentication server and incorporating means for initiating communication with a credit card user in response to the received order, requesting a predefined verification code from the user and means for identifying an authentic verification code to enable processing of the transaction.

20. A processing system as claimed in claim 19 in which the means first authentication server incorporates processing means for detecting a card not present flag in the received order and for controlling communication between the first and second authentication servers using the detected card not present flag.

21. A processing system as claimed in claim 19 or claim 20 in which the second authentication server incorporates a computer telephony interface (CTI) for automatic communication with the credit card user using unique predefined communication data stored in the second authentication server.

22. A processing system as claimed in claim 21 in which the computer telephony interface is formed for generation of an audio message for transmission to the credit card user.

23. A processing system as claimed in any of claims 19 to 22 in which the means for identifying an authentic verification code incorporates means for receiving a personal identification number (PIN) from the credit card user and means for comparing the received PIN with a predefined PIN stored on the second authentication server.

24. A processing system as claimed in claim 23 in which, the second authentication server incorporates means for automatically generating an authentication code in response to a matched PIN condition based on, a user identifier, a vendor identifier,

timestamp and transaction value.

25. A processing system as claimed in any of claims 19 to 24 in which the means for controlling communication between the authentication server and a credit card user in response to the order further incorporates means for generating a response telephone box and for communicating a telephone box location to the credit card user.

26. A processing system for verification of credit card transactions, having a vendor interface for receiving an order from a vendor and means for authenticating legitimacy of the received order, characterised in that the means for authenticating legitimacy of the received order incorporates means for generating an authentic verification code to enable processing of the order by requesting and receiving a predefined code from a user, the authentic verification code incorporating timestamp information and being independent of the predefined code.

27. A user interface for use in the verification of credit card transactions, for receiving an order from a vendor and means for authenticating legitimacy of the received order, characterised in that the means for authenticating legitimacy of the received order incorporates means for generating an authentic verification code to enable processing of the order by requesting and receiving a predefined code from a user, the authentic verification code incorporating timestamp information and being independent of the predefined code.

28. A communications interface for verification of credit card transactions incorporating: -

means for receiving an authentication request in response to an order;

means for identifying a user from the authentication request; and

means for generating an authentic verification code to enable processing of

the order by requesting and receiving a predefined code from the identified user.

5

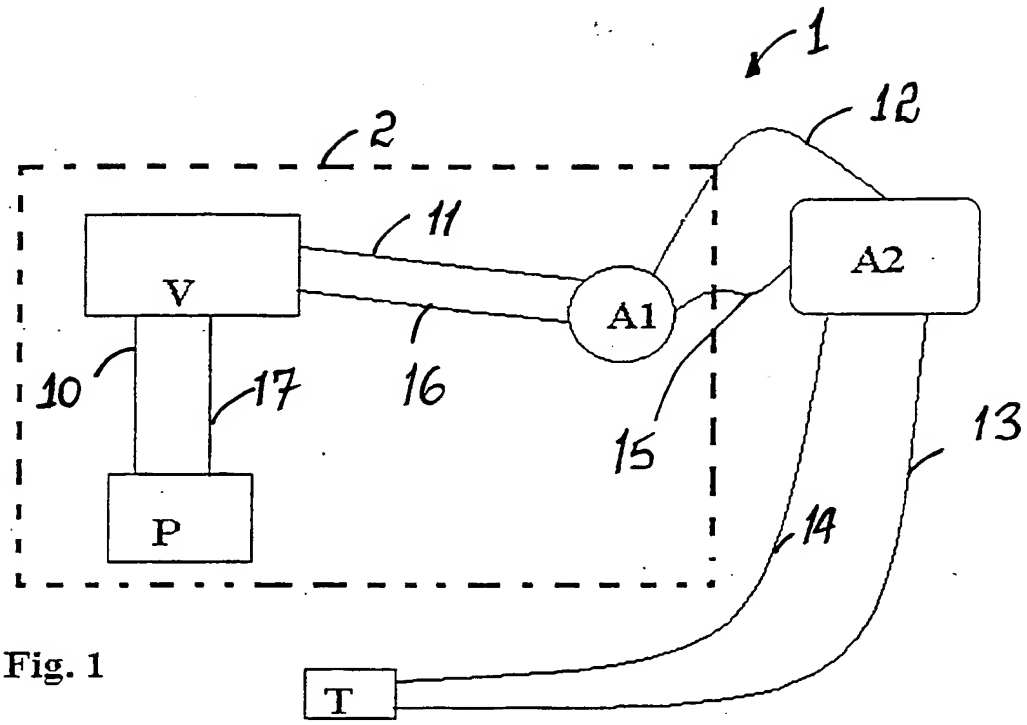
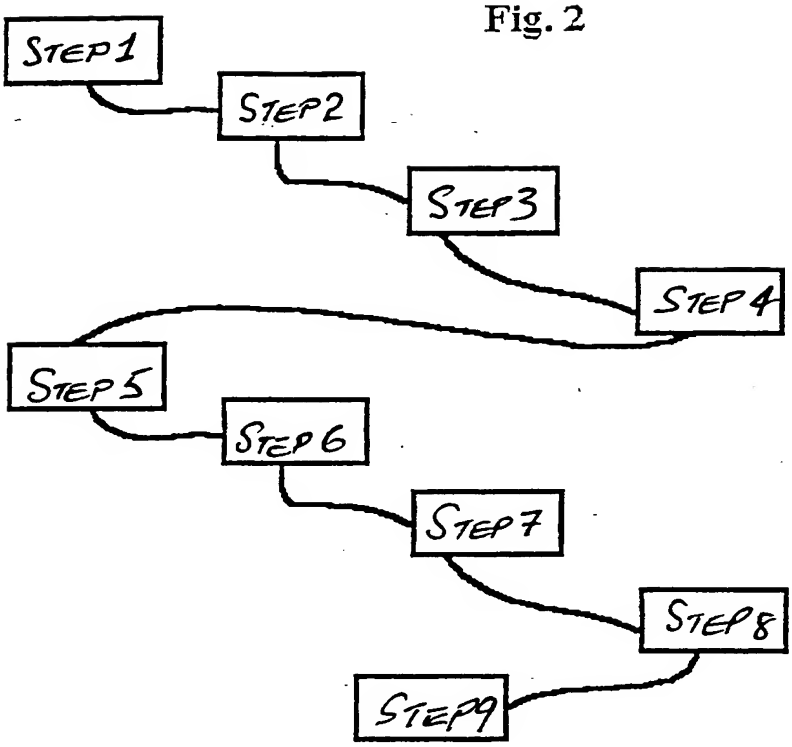


Fig. 1

Fig. 2



INTERNATIONAL SEARCH REPORT

ernational Application No
PCT/IE 01/00004

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 745 961 A (AT & T CORP) 4 December 1996 (1996-12-04) column 6, line 49 -column 8, line 38 column 9, line 51 -column 10, line 36 column 13, line 46 -column 16, line 31 ---	1-4,7, 12-15, 18-22, 25,28
A	WO 99 23617 A (KREMER GILLES ;CHANUDET PATRICK (FR)) 14 May 1999 (1999-05-14) page 13, line 11 -page 20, line 27 page 24, line 16 -page 26, line 19 page 30, line 4 -page 35, line 33 page 44, line 15 -page 45, line 7 --- -/--	1-6, 9-17,19, 21-24, 26-28

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 May 2001	11/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bocage, S

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

`ernational Application No
PCT/IE 01/00004

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 05, 31 May 1999 (1999-05-31) & JP 11 045366 A (ATENSHIYON SYST KK), 16 February 1999 (1999-02-16) abstract	1,12,19, 28
A	EP 0 416 482 A (HITACHI LTD) 13 March 1991 (1991-03-13) column 4, line 46 -column 5, line 10 column 6, line 46 -column 7, line 14 column 11, line 6 - line 44 column 18, line 15 - line 27	1,3,4
A	DE 197 18 103 A (SCHMITZ KIM) 4 June 1998 (1998-06-04)	
A	WO 97 39565 A (ROZETTI MAKS) 23 October 1997 (1997-10-23)	
A	US 5 742 684 A (LABATON ISAAC ET AL) 21 April 1998 (1998-04-21)	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

ernational Application No
PCT/IE 01/00004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0745961 A	04-12-1996	US 5708422 A	13-01-1998
		CA 2176163 A,C	01-12-1996
		JP 8339407 A	24-12-1996
WO 9923617 A	14-05-1999	FR 2771875 A	04-06-1999
		AU 1158899 A	24-05-1999
		EP 1050025 A	08-11-2000
JP 11045366 A	16-02-1999	JP 3103327 B	30-10-2000
EP 0416482 A	13-03-1991	JP 3179863 A	05-08-1991
		DE 69023843 D	11-01-1996
		DE 69023843 T	13-06-1996
		US 5315634 A	24-05-1994
DE 19718103 A	04-06-1998	AU 6354598 A	05-11-1998
		BR 9801177 A	20-03-2001
		CN 1207533 A	10-02-1999
		EP 0875871 A	04-11-1998
		JP 10341224 A	22-12-1998
		US 6078908 A	20-06-2000
WO 9739565 A	23-10-1997	US 5745554 A	28-04-1998
		AU 2439897 A	07-11-1997
US 5742684 A	21-04-1998	IL 100238 A	24-01-1995
		US 5524072 A	04-06-1996
		CA 2125193 A	10-06-1993
		EP 0615673 A	21-09-1994
		JP 7505023 T	01-06-1995
		WO 9311619 A	10-06-1993